https://www.wsj.com/articles/fraud-case-in-charleston-s-c-shines-light-on-webs-dark-corners-11581944400

◆ WSJ NEWS EXCLUSIVE | U.S.

Fraud Case in Charleston, S.C., Shines Light on Web's Dark Corners

Micfo and its founder pleaded not guilty in case revolving around IP addresses and the American Registry for Internet Numbers

By Byron Tau Follow *and Dustin Volz* Follow

Feb. 17, 2020 8:00 am ET

Amir Golestan and his company, Micfo, face 20 counts of wire fraud in a case brought in U.S. District Court in South Carolina. PHOTO: MICFO

CHARLESTON, S.C.—A first-of-its-kind fraud prosecution of a small technology company and its owner has shed light on how the architecture of the internet

allows spammers, hackers and other bad actors to flourish online while cloaking their true identities.

Amir Golestan and his company, Micfo—a web-services provider based above a cafe in a building in this city's historic district—face 20 counts of wire fraud in a case brought in U.S. District Court in South Carolina. Both Mr. Golestan and the corporation have pleaded not guilty.

The alleged victim: the American Registry for Internet Numbers, a Centreville, Va., nonprofit that assigns internet protocol addresses in North America and the Caribbean to all online devices.

It is the first such federal case alleging fraud involving internet resources, and it could determine new boundaries for criminal behavior within the loosely regulated world of internet infrastructure.

The case revolves around IP addresses, which allow devices to communicate with each other online.

Most consumers are automatically assigned an IP address to get online through a cellphone or internet service provider; companies might use thousands for their technology platforms. Because the addresses are the online equivalent of home phone numbers, they are key identifiers for law-enforcement authorities pursuing online crime.

In the Micfo case, filed last May, the Justice Department alleges Mr. Golestan created shell companies solely to deceive the registry into granting him 800,000 IP addresses—which he would have struggled to obtain by other means, especially as the most common type of new IP addresses has become scarce. Mr.

Golestan then leased or sold those addresses to clients, according to the complaint and his own account.

Many of the clients were Virtual Private Networks, known as VPNs, which give users anonymity. VPNs are widely used for purposes such as protecting online privacy or allowing dissidents to operate under oppressive regimes. But they also are used by people who transmit illicit content or engage in cybercrime to hide their tracks—and require large numbers of IP addresses to enable users to mask their Web traffic.

As Micfo amassed VPN clients using the IP addresses it had allegedly obtained illegitimately, a huge amount of traffic—some of it illicit or criminal—passed through its computer servers but wasn't traceable to the true originators, according to government subpoenas directed at Micfo and reviewed by The Wall Street Journal.

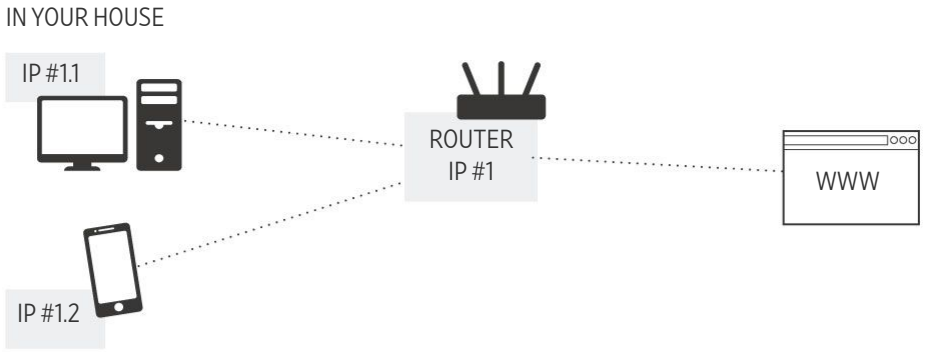
The charges don't allege that Mr. Golestan and Micfo were part of or aware of illegal activity transmitted via VPNs through Micfo's servers. Rather, the Justice Department charged him and the company with defrauding the internet registry to obtain the IP addresses over a period of several years.

Prosecutors placed a value of $14 million on Mr. Golestan's alleged scheme, based on the government's estimated value of between $13 and $19 for each address in the secondary market, according to the court complaint.

Scarce Addresses

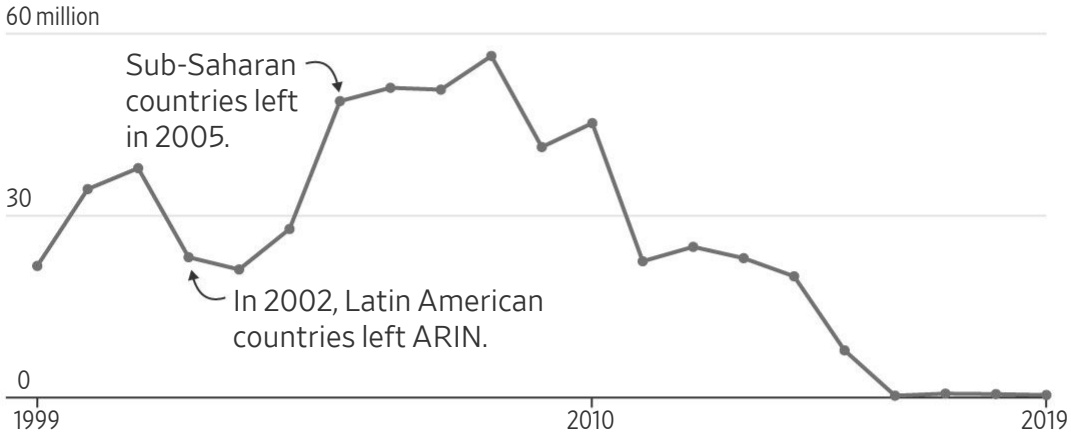
An IP is a unique number that identifies each device connected to the internet and allows different gadgets to communicate with each other. An IPv4 is generated by combining four

numbers (each of them ranging from 0 to 255), with more than four billion possible outcomes. Most of these combinations are already in use.

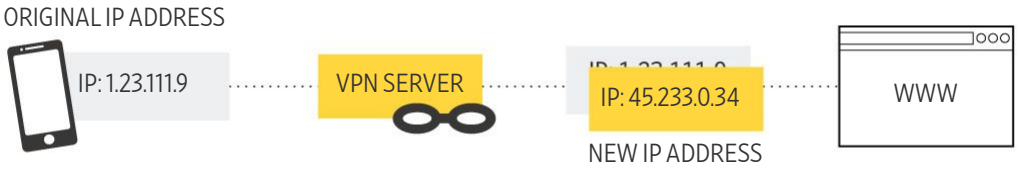


In the case of the U.S., Canada and parts of the Caribbean, the few IPv4 addresses remaining are allocated by the American Registry for Internet Numbers, or ARIN, a U.S. nonprofit.

IPv4 addresses issued by ARIN since 1999

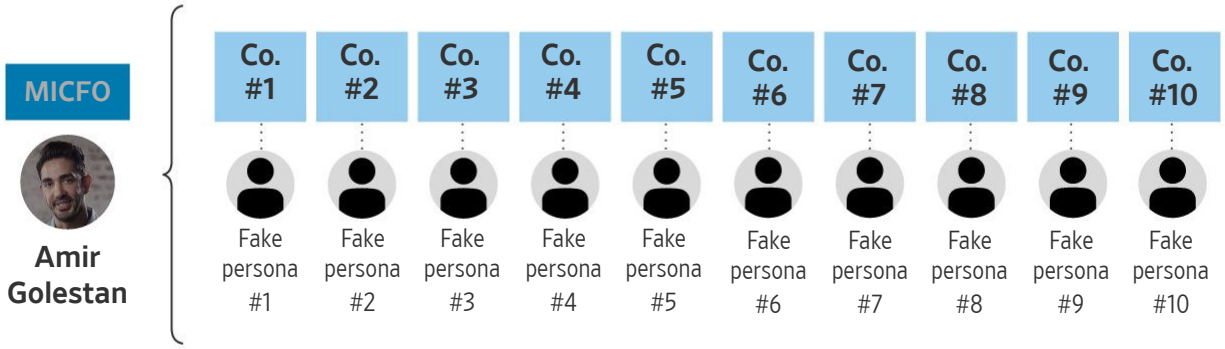


Prosecutors allege Micfo obtained hundred of thousands of IPv4 addresses illegally. This company provides internet services, mostly to other companies that offer Virtual Private Networks (VPN), a service that helps to hide the device's IP and location and makes it harder to track what users do on the internet.

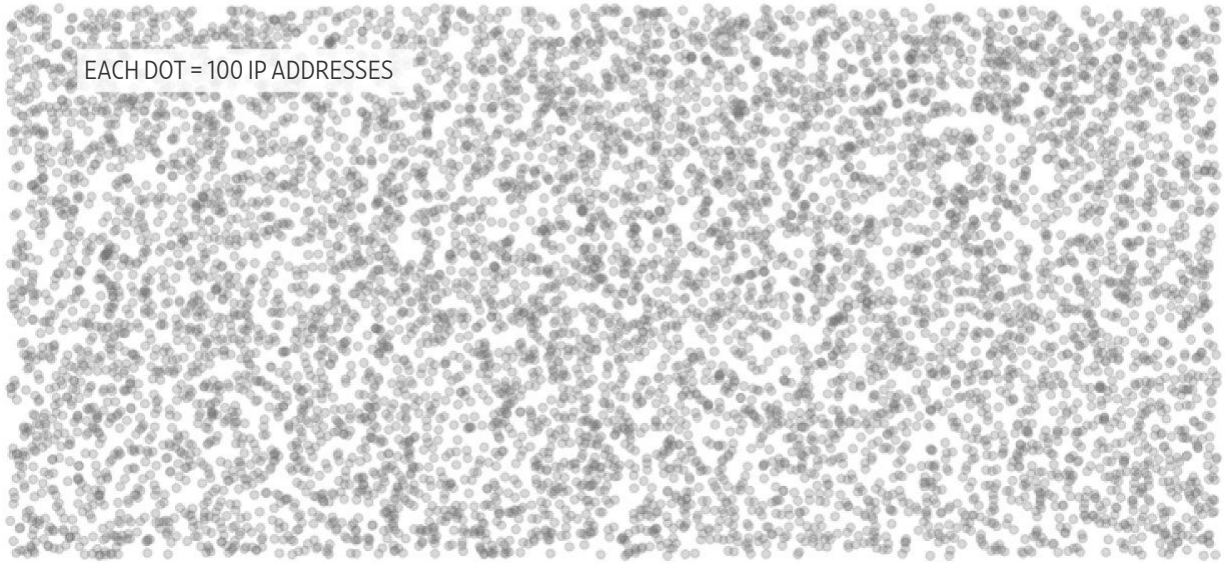


A NETWORK OF SHELL COMPANIES

Micfo's CEO, Amir Golestan, created a network of shell companies with fake personas, with names like "Kevin Chang" and "Jonathan Lieberman."



Using these companies, Micfo purchased nearly 800,000 IPv4 addresses worth $14 million—far more addresses than the company could have purchased without the fake companies.



Some of those IPs were rented or sold to VPN clients. In some cases, the VPN's customers engaged in illegal practices, including spam and viewing child pornography.

Sources: American Registry for Internet Numbers (ARIN) and court records
Luis Melgar/THE WALL STREET JOURNAL

Mr. Golestan, in an interview, acknowledged creating 10 fictitious personas to pose as chief executives of 10 shell entities to obtain the IP addresses he then used to build his business.

But he said he broke no law and was engaged in the "victimless" use of pseudonyms to provide a service. "It comes with the territory of this industry," he said. Born in Iran, Mr. Golestan, 36 years old, started Micfo in 1999 in the bedroom of his childhood home in Dubai before emigrating to the U.S.

IP addresses that Micfo obtained and leased to others have cropped up in many law-enforcement investigations: Former employees said in interviews, and Mr. Golestan confirmed, that Micfo was inundated with subpoenas and other legal requests from around the world tied to probes that traced information to its servers.

A sample of requests received by Micfo and reviewed by the Journal showed law-enforcement requests for material related to terrorist threats, child pornography, hacking and other alleged criminal activity.

Micfo was rarely able to produce detailed records to law enforcement, several former employees said. Micfo didn't have any information beyond the IP address and which VPN clients were leasing them.

Mr. Golestan said receiving subpoenas was part of the routine business of hosting internet traffic for VPN companies. Some former employees said Mr.

Micfo headquarters in Charleston, S.C. PHOTO: BYRON TAU/THE WALL STREET JOURNAL

Golestan discouraged them from cooperating fully with subpoena demands. Mr. Golestan denied doing that and said Micfo complied with all lawful demands from law enforcement.

Private investigators looking at hacks of emails and other online accounts of two prominent Americans—Therese Shaheen, a former top U.S. envoy to Taiwan, and Elliott Broidy, a former Trump fundraiser—allege they were carried out through VPN clients of Micfo using IPs owned by the company.

Mr. Golestan said he had no knowledge of those incidents. He said Micfo provides a legitimate service to VPNs, adding that whatever his customers or their users do through Micfo servers is none of his business. "You can buy a knife to chop a tomato—or you can buy a knife to kill someone," he told employees on the day he was indicted in May 2019, someone who was there said.

Amassing IP addresses has become a lucrative business because the American internet registry and its counterparts around the world are running out of unique addresses—or at least the current version, IPv4, of which there are about four billion. A switch to the next generation is under way, which will make billions more addresses available, but it will take years to complete.

The American internet registry, which requires companies to demonstrate a need for new IP addresses, said it had no idea Mr. Golestan was creating phony companies to apply.

The registry and its counterparts historically have done little to vet entities requesting IP addresses, because for years they were plentiful and the emphasis was on advancing global internet connectivity, experts said. "This is the system, as it has been cobbled together out of odd bits and pieces, over the past 30-plus years," said Ron Guilmette, a California-based internet-fraud investigator. "It has clearly not aged well." Funding for the registry and others like it come from the fees companies pay for IP services.

The American Registry for Internet Numbers said it watches for fraud and pressed the Federal Bureau of Investigation to investigate Micfo when it discovered a change in ownership of two identical blocks of IP addresses—one owned by Micfo and one traced to one of Mr. Golestan's shell companies.

John Curran, president of the registry, said, "While recognizing this is the first prosecution of its kind, it sends a strong reminder of potential criminal liability for those who consider hijacking number resources or obtaining them through fraud."

Mr. Golestan said he had no choice but to use shell companies to obtain additional IP addresses. The registry cut Micfo off from getting new addresses in 2013, suspecting he was engaged in fraud, a person familiar with the matter said. Around the same time, the nonprofit watchdog group SpamHaus placed Micfo on a "blocklist" of companies that allow known spammers to use their networks,

which blocked Micfo's IP companies' access to major tech platforms for outgoing email.

To grow, Mr. Golestan said, Micfo began catering to VPNs. He contends the American internet registry has too much power and can make arbitrary decisions on the granting of IP addresses. "They don't report to anybody and they are untouchable," he said.

Former employees described extensive efforts by Micfo to make its phony companies look convincing.

According to documents reviewed by The Journal, Mr. Golestan created shell companies with names like "Contina," "HostAware" and "OppoBox," made up fictitious executives and set up dummy email accounts. He registered virtual office space and created websites using stock photos to make the shell companies appear legitimate. He kept a record of the personas and companies in a spreadsheet he titled "G77."

Employees were kept in the dark, several former workers said. They believed the companies were real businesses that Micfo partnered with. Some reported communicating by email with a "Kevin Chang," purportedly an executive from OppoBox, but he didn't exist. Nor did "Jonathan Lieberman," "Yong Wook-Kwon," "Pooya Torabi" or "Steve Cunningham."

Mr. Golestan likened the use of fake businesses to how call-center employees abroad sometimes adopt Americanized names—a harmless deception.

Those fake companies secured blocs of IP addresses from the registry. And they served another purpose, Mr. Golestan said: to disguise the ownership of the IP

blocks from the VPN clients, who typically don't want to rely heavily on any single company for IP addresses and Web servers.

Mr. Golestan said in the interview that the registry of internet numbers was paid properly for the blocs of IP addresses and so can't have been defrauded.

A lawyer for the registry dismissed that argument as "factually and legally irrelevant."

As evidence that he runs a legitimate business, Mr. Golestan showed documents to the Journal describing FBI efforts to cultivate him in 2018 as a confidential source on hacking and international terrorism investigations. Mr. Golestan said that in interviews with agents he was largely unable to provide any leads. The FBI declined to comment.

Since the charges were filed, most of Micfo's employees have quit, and many of its longtime clients have left. Mr. Golestan said he plans to go to trial, though no date has been set. "We are going to go fight," he said.

Write to Byron Tau at byron.tau@wsj.com and Dustin Volz at dustin.volz@wsj.com

Appeared in the February 18, 2020, print edition.